IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DESMOND GARMON, ZELL HATHORNE, LEWIS HOBBY, JR., BENNIE REED, RHANAE GREER, SUNSHINE SMITH, ANTWON CHERRY, CHARISSE LANGSTON, and LATONIA ADAMS, Plaintiffs, vs. **RALPHS GROCERY COMPANY, d/b/a FOOD 4 LESS MIDWEST, and THE KROGER CO.,** Defendants.	Case Nos.: **1:23-cv-15345** (consolidated with 1:24−cv−01898) Honorable Steven C. Seeger **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT

DESMOND GARMON, ZELL HATHORNE, LEWIS HOBBY, JR., BENNIE REED, RHANAE GREER, SUNSHINE SMITH, ANTWON CHERRY, CHARISSE LANGSTON, and LATONIA ADAMS (collectively "Plaintiffs"), through counsel, for their First Amended Complaint against Defendants, RALPHS GROCERY COMPANY, d/b/a FOOD 4 LESS MIDWEST ("Food 4 Less"), and THE KROGER CO. ("Kroger") (collectively "Defendants"), their subsidiaries and affiliates, state:

NATURE OF THE CASE

1. This is an action to recover statutory damages and for injunctive relief arising out of Defendants' unlawful collection, receipt, use, possession, retention and disclosure of the personal biometric identifiers and biometric information of Plaintiffs in violation of the Biometric Information Privacy Act ("BIPA"), 740 ILCS § 14/1 (2008).

THE PARTIES

2. Each Plaintiff is a natural person and is domiciled in Illinois.

3. Defendant Ralphs Grocery Company d/b/a Food 4 Less Midwest is an Ohio corporation with its principal place of business located at 1100 W. Artesia Blvd., Compton, CA 90220. Defendant is registered with the Illinois Secretary of State and conducts business in the State of Illinois.

4. Defendant The Kroger Co. is an Ohio corporation with its principal place of business located at 1014 Vine Street, Cincinnati, OH 45202. Defendant is registered with the Illinois Secretary of State and conducts business in the State of Illinois.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a) as the matter in controversy exceeds $75,000.00[1] exclusive of punitive damages, and/or interest and costs, and is between citizens of different States.

6. Each Plaintiff is a citizen of Illinois.

7. Each Defendant is a foreign corporation with its principal place of business located in another state.

8. This Court has personal jurisdiction over Defendants because they conduct substantial business in Illinois.

9. Venue lies in this District pursuant to 28 U.S.C. §1391(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District and Defendants can be found in this District.

RELEVANT FACTS

[1]Plaintiffs seek statutory, liquidated damages of $1,000 for each negligent violation of BIPA and $5,000 for each intentional or reckless violation of BIPA and allege that there were not less than 19,370 BIPA violations.

10. Food 4 Less is a grocery store chain in the "Kroger Family of Companies" and is a subsidiary of Kroger.[2]

11. Kroger ranks as one of the world's largest retailers, operating nearly 2,800 stores in 35 states and the District of Columbia with annual sales of more than $132.5 billion. Kroger serves nearly 11 million customers a day.[3]

12. From 2018 to the present, Defendants have operated grocery stores in Illinois under the "Food 4 Less" banner, including the following locations:

a. 2501 W. North Ave., Melrose Park, IL 60160
b. 1000 E. Sibley Blvd.., Dolton, IL 60419
c. 112 W. 87th Street, Chicago, IL 60620
d. 4821 W. North Avenue, Chicago, IL 60639
e. 4620 S. Damen Ave., Chicago, IL 60609 – closed
f. 7770 S. Cicero Ave., Burbank, IL 60459 – closed
g. 5556 159th Street, Oak Forest, IL 60452 – closed

13. Each Plaintiff is or was employed at one or more of the Food 4 Less locations.

14. Food 4 Less stores are Kroger family stores.

15. When Plaintiffs were initially hired by Food 4 Less, they were required to enroll in a biometric timekeeping system (time clock and timekeeping databases) using a scan of their fingerprint.[4] Plaintiffs were to scan, upload and/or use their unique fingerprint in order to use the biometric timekeeping system utilized by the Kroger family stores, including Food 4 Less.

16. Defendants' policies required Plaintiffs each to use their fingerprint to clock in and clock out at the beginning and end of each shift and for meal breaks.[5]

---

[2] *See* https://www.food4less.com/i/kroger-family-of-companies (last accessed 10/26/2023).
[3] *See* https://www.thekrogerco.com/about-kroger/ (last accessed 10/26/2023).
[4] Fingerprint also means thumbprint.
[5] *Maetean Johnson v. Ralphs Grocery Company d/b/a Food 4 Less Midwest, and The Kroger Co.,* was originally filed on March 25, 2022 in the Circuit Court of Cook County, IL (Case No. 2022CH02683) and removed to the Northern District of Illinois, Eastern Division on May 6, 2022 (Case No. 1:22-cv-02409). Any Plaintiffs who were members of that settlement class have excluded themselves.

17. Kroger family stores, including Food 4 Less, have used software that required workers to use fingerprints as a means of authentication.

18. Kroger's family stores, including Food 4 Less, collected and/or otherwise obtained and stored Plaintiffs' biometric data upon Plaintiffs' initial enrollment in the biometric timekeeping system for purposes of time tracking and employee authentication.

19. Alternatively, Defendants' biometric timekeeping system used, collected, and stored an encrypted mathematical representation of each Plaintiff's specific fingerprint or hand geometry characteristics for purposes of time tracking and employee authentication.

20. In either event, Defendants' timekeeping system used, collected, and stored unique "biometric identifiers" and "biometric information," as both terms are defined below, belonging to each Plaintiff.

21. Defendants' biometric timekeeping system (time clock and timekeeping databases) tracks data in real time, including each time the Plaintiffs clocked in and out.

22. Plaintiffs' data collected in the biometric timekeeping system by Food for Less was disclosed to at least one third-party for payroll purposes.

23. Plaintiffs' data collected in the biometric timekeeping system by Food for Less was disclosed to Kroger.

24. While there are tremendous benefits to using biometric time clocks in the workplace, there are also serious risks. Unlike key fobs or identification cards—which can be changed or replaced if stolen or compromised—fingerprints or scans of fingers--are unique, permanent biometric identifiers associated with the employee. This exposes employees to serious and irreversible privacy risks. For example, if a fingerprint database is hacked, breached, or otherwise exposed, employees have no means by which to prevent identity theft and unauthorized

tracking. If a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Yahoo, eBay, Equifax, Uber, Home Depot, MyFitnessPal, Panera, Whole Foods, Chipotle, Omni Hotels & Resorts, Trump Hotels, and Facebook/Cambridge Analytica data breaches or misuses – employees have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

25. A nefarious market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018; last assessed 09/19/2023).

26. In 2015, a hacking event of the U.S. Office of Personnel Management caused 5.6 million people's fingerprints to compromised. *See* April Glaser, *Biometrics Are Coming, Along with Serious Security Concerns*, WIRED (Mar. 9, 2016; last assessed 09/19/2023).

27. By 2019, biometrics were expected to become a 25-billion-dollar industry with more than 500 million biometric scanners in use around the world. Chiara A. Sottile, *As Biometric Scanning Use Grows, So Does Security Risk*, NBC NEWS: MACH (July 24, 2016, 6:29 PM; last assessed 09/19/2023).

28. The use of biometric information for timekeeping has become so common in an employment setting as to be almost ubiquitous. Companies use biometric devices as a more secure way to authenticate employee identity for timekeeping, to grant access to sensitive data, or to facilitate onboarding and offboarding. Companies use biometric systems to ensure that workers using a time clock are who they say they are and to avoid "buddy punching." Biometric time clocks

that use fingerprint scanning or facial recognition can also help companies better comply with labor laws by ensuring employees clock in and out accurately. *See* Jay Hux, *Collecting Employee Biometric Data Could Prove Costly in Illinois*, SHRM: ST. & LOC. UPDATES (Sept. 19, 2017).

29. On May 18, 2023, the Federal Trade Commission voted 3-0 and adopted a new policy statement on Biometric Information and Section 5 of the Federal Trade Commission Act.[6] The decision to adopt the new policy reflects the FTC's significant concerns about biometric information and related technologies with respect to privacy, security and other issues.

30. In commenting on the above policy statement, Samuel Levine, Director of the FTC's Bureau of Consumer Protection, said: "In recent years, biometric surveillance has grown more sophisticated and pervasive, posing new threats to privacy and civil rights," "Today's policy statement makes clear that companies must comply with the law regardless of the technology they are using."[7]

31. Recognizing the need to protect its citizens from situations like these, in 2008, Illinois enacted BIPA in light of the "very serious need [for] protections for the citizens of Illinois when it comes to [their] biometric information."[8]

32. BIPA was enacted with the understanding that "the full ramifications of biometric technology are not fully known." 740 ILCS § 14/5(f). The legislature specifically found that persons who have their biometrics taken unlawfully are at increased risk of future injury. *Id.*

33. Biometrics are unlike other unique identifiers used to access finances or other sensitive information. "For example, social security numbers, when compromised, can be changed.

---

[6] *See* https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf (last accessed 10/26/2023)

[7] *See* https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers (last accessed 10/26/2023)

[8] 95th Ill. Gen. Assem. House Proceedings, May 30, 2008, at 249 (statement of Representative Ryg), available at http://www.ilga.gov/house/transcripts/htrans95/09500276.pdf.

Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[9]

34. To address this legitimate concern, Section 15(b) of BIPA provides that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.[10]

35. For BIPA purposes, a "biometric identifier" is a personal feature that is unique to an individual and specifically includes fingerprints. 740 ILCS § 14/10.

36. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based upon an individual's biometric identifier used to identify the individual." *Id.*

37. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it *first*:

[9] 740 ILCS § 14/5(c).
[10] 740 ILCS § 14/15(b).

> (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS § 14/15(b).

38. BIPA specifically applies to employees who work in the State of Illinois.

39. BIPA defines a "written release" specifically "in the context of employment [as] a release executed by an employee as a condition of employment." 740 ILCS § 14/10.

40. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an identifier that is used to identify an individual. *See id*.

41. BIPA also establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information. *See* 740 ILCS § 14/15(c)-(d). BIPA makes it unlawful for companies to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." Furthermore, no company may "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless":

> (1) the person or customer consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the person or customer;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

See 740 ILCS § 14/15(c)-(d).

42. Ultimately, BIPA is an informed consent statute. Its narrowly tailored provisions place no absolute bar on collecting, sending, transmitting or communicating of biometric data. For example, BIPA does not limit what kinds of biometric data may be collected, sent, transmitted, or stored. Nor does BIPA limit from whom biometric data may be collected, to whom it may be sent, transmitted, or stored. BIPA merely mandates that entities wishing to engage in that conduct must make proper disclosures and implement certain reasonable safeguards.

FACTS RELATED TO PLAINTIFFS

43. Plaintiff Desmond Garmon ("Garmon") has been continuously employed by Defendants at the Food 4 Less store located at 2501 W. North Avenue, Melrose Park, Illinois, from February 2022 to the present.

44. In approximately mid-summer 2023, Defendants discontinued utilizing the biometric time clock system at the Melrose Park Food 4 Less store.

45. From February 2022 to approximately mid-summer 2023, Garmon was required to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

46. After the *Johnson* class action was filed on March 25, 2022, Defendants recklessly and intentionally continued to utilize the biometric time clock system and until approximately mid-summer 2023, requiring Garmon to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

47. From February 2022 to approximately mid-summer 2023, Garmon scanned his fingerprint to clock in or clock out of Defendants' biometric time clock system no less than four times each working day.

48. From February 2022 to approximately mid-summer 2023, Garmon utilized Defendants' biometric time clock system at least 1,300 times.

49. Plaintiff Zell Hathorne ("Hathorne") has been continuously employed by Defendants as a part-time employee at the Food 4 Less store located at 1000 Sibley Blvd., Dolton, Illinois, from August 2016 to the present.

50. In approximately mid-summer 2023, Defendants discontinued utilizing the biometric time clock system at the Dolton Food 4 Less store.

51. From August 2016 to approximately mid-summer 2023, Hathorne was required to scan his fingerprint each time he began and ended his working day, and when Hathorne clocked in and out for breaks.

52. After the *Johnson* class action was filed on March 25, 2022, Defendants recklessly and intentionally continued to utilize the biometric time clock system and, until approximately mid-summer 2023, requiring Hathorne to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

53. From August 2016 to approximately mid-summer 2023, Hathorne scanned his fingerprint to clock in or clock out of Defendants' biometric time clock system no less than two times each working day.

54. From approximately mid-summer 2018 until approximately mid-summer 2023, Hathorne utilized Defendants' biometric time clock system at least 1,200 times.

55. Plaintiff Lewis Hobby, Jr. ("Hobby") was employed by Defendants at the Food 4 Less store in Dolton, Illinois from July 2017 to August 2021.

56. From July 2017 to August 2021, Hobby was required to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

57. At all times during his employment, Hobby scanned his fingerprint to clock in or clock out of Defendants' biometric time clock system no less than four times each working day.

58. From July 2017 to August 2021, Hobby utilized Defendants' biometric time clock system at least 3,000 times.

59. Plaintiff Bennie Reed ("Reed") has been continuously employed by Defendants as a part-time employee at Food 4 Less stores from April 29, 2022 to the present.

60. Reed was originally employed at the Food 4 Less store located at 5556 159th Street, Oak Forest, Illinois until the store was closed. Since the closing of that store, Reed has been continuously employed at the Dolton, Illinois Food 4 Less store.

61. In approximately mid-summer 2023, Defendants discontinued utilizing the biometric time clock system at the Dolton Food 4 Less store.

62. From April 29, 2022 to approximately mid-summer 2023, Reed was required to scan her fingerprint each time she began and ended her working day, as well as each time she clocked in and out for breaks.

63. Although the *Johnson* class action was filed on March 25, 2022, before Reed was employed at Food 4 Less, Defendants required Reed to enroll in Defendants' biometric timekeeping system (time clock and timekeeping databases) using a scan of her fingerprint. Defendants recklessly and intentionally continued to utilize the biometric time clock system, and

until approximately mid-summer 2023, requiring Reed to scan her fingerprint each time she began and ended her working day, as well as each time she clocked in and out for breaks.

64. From April 29, 2022 to approximately mid-summer 2023, Reed scanned her fingerprint to clock in or clock out of Defendants' biometric time clock system no less than two times each working day.

65. From April 29, 2022 until approximately mid-summer 2023, Reed utilized Defendants' biometric time clock system at least 500 times.

66. Plaintiff Rhanae Greer ("Greer") was employed by Defendants at Food 4 Less stores from August 2018 to March 2022.

67. Greer was originally employed at the Food 4 Less store located at 7770 S. Cicero Avenue, Burbank, Illinois until the store was closed in mid-2019. After the closing of that store, Greer was continuously employed at Food 4 Less store located at 112 W. 87th Street, Chicago, Illinois until March 2022.

68. From August 2018 to March 2022, Greer was required to scan her fingerprint each time she began and ended her working day, as well as each time she clocked in and out for breaks. In her position as a front-end lead, Greer was also required to scan her fingerprint each time she had to override punches for employees.

69. At all times during her employment, Greer scanned her fingerprint to clock in or clock out of Defendants' biometric time clock system and to override employees' punches no less than ten times each working day.

70. From August 2018 to March 2022, Greer utilized Defendants' biometric time clock system at least 2,000 times.

71. Plaintiff Sunshine Smith ("Smith") has been continuously employed by Defendants at the Dolton, Illinois Food 4 Less store from August 2016 to the present.

72. In approximately mid-summer 2023, Defendants discontinued utilizing the biometric time clock system at the Dolton Food 4 Less store.

73. From August 2016 to August 2023, Smith was required to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

74. After the *Johnson* class action was filed on March 25, 2022, Defendants recklessly and intentionally continued to utilize the biometric time clock system and until approximately mid-summer 2023, requiring Smith to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks.

75. From August 2016 to approximately mid-summer 2023, Smith scanned his fingerprint to clock in or clock out of Defendants' biometric time clock system no less than four times each working day.

76. From approximately mid-summer 2018 to approximately mid-summer 2023, Smith utilized Defendants' biometric time clock system at least 4,800 times.

77. Plaintiff Antwon Cherry ("Cherry") was employed by Defendants at the Food 4 Less store in Dolton, Illinois from September 29, 2008 to February 26, 2023.

78. During his employment, Cherry was required to scan his fingerprint each time he began and ended his working day, as well as each time he clocked in and out for breaks. Cherry was also required to scan his fingerprint each time he had to override punches for co-workers.

79. After the *Johnson* class action was filed on March 25, 2022, Defendants recklessly and intentionally continued to utilize the biometric time clock system and until February 26, 2023, requiring Cherry to scan his fingerprint each time he began and ended his working day, as well as

each time he clocked in and out for breaks, and each time he had to override punches for co-workers.

80. During his employment, Cherry scanned his fingerprint to clock in or clock out of Defendants' biometric time clock system and to override employees' punches no less than four times each working day.

81. From February 26, 2018 to February 26, 2023, Cherry utilized Defendants' biometric time clock system at least 4,800 times.

82. Plaintiff Charisse Langston ("Langston") was employed by Defendants as a part-time employee at the Food 4 Less store located at 4821 W. North Avenue, Chicago, Illinois, from November 2021 to May or June 2023.

83. During her employment, Langston was required to scan her fingerprint each time she began and ended her working day.

84. After the *Johnson* class action was filed on March 25, 2022, Defendants recklessly and intentionally continued to utilize the biometric time clock system and, until April 2023, required Langston to scan her fingerprint each time she began and ended her working day.

85. During her employment, Langston scanned her fingerprint to clock in or clock out of Defendants' biometric time clock system no less than two times each working day.

86. From November 2021 to April 2023, Langston utilized Defendants' biometric time clock system at least 470 times.

87. Plaintiff Latonia Adams ("Adams") was employed by Defendants at the Food 4 Less store located at 2501 W. North Avenue, Melrose Park, Illinois, (the "Melrose Park Location") from February 2020 to July 2021.

88. From February 2020 to approximately July 2021, Adams was required to scan her fingerprint each time she began and ended her working day, as well as each time she clocked in and out for breaks.

89. From February 2020 to approximately July 2021, Adams scanned her fingerprint to clock in or clock out of Defendants' biometric time clock system no less than four times each working day.

90. From February 2020 to approximately July 2021, Adams utilized Defendants' biometric time clock system at least 275 times.

91. Neither Defendant informed Plaintiffs of the specific limited purposes or length of time for which the Defendants collected, stored, or used Plaintiffs' biometric identifier or biometric information.

92. Similarly, neither Defendant ever informed Plaintiffs of any biometric data retention policy it developed, nor whether it will ever permanently delete their biometric information.

93. Plaintiffs never signed a written release allowing either Defendant to collect, capture, or otherwise obtain their biometric information.

94. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendants' repeated violations of BIPA alleged herein.

95. Each Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems that Defendants used would be subject to the provisions of BIPA, a law in effect since 2008, yet wholly failed to comply with the statute.

96. Furthermore, when the *Johnson* class action was filed on March 25, 2022, each Defendant knew that the biometric timekeeping systems that Defendants used would be subject to

the provisions of BIPA, yet recklessly and intentionally continued to utilize the biometric timekeeping systems until approximately mid-summer 2023, requiring employees to use their fingerprint to clock in and clock out at the beginning and end of each working day, as well as each time they clocked in and out for breaks.

97. Alternatively, each Defendant negligently failed to comply with BIPA by failing to adhere to the reasonable standard of care in its industry with respect to employee biometric identifiers or information. 740 ILCS § 14/15(e).

98. Plaintiffs now seek statutory, liquidated damages under BIPA as compensation for the Defendants' multiple violations of BIPA.

99. Plaintiffs Garmon, Hathorne, Reed, Smith, Cherry, and Langston, seek liquidated damages of $5,000 for *each* intentional and/or reckless violation of BIPA specifically for the period from March 25, 2022 to approximately mid-summer 2023.

100. Plaintiffs also seek a declaration that Defendants' actions in contravention of BIPA are unlawful and to enjoin Defendants from further violations of BIPA.

101. This lawsuit constitutes Plaintiffs' one and only chance at compensation for Defendants' violations of BIPA. Depending on how technology evolves years into the future, losing control of and ownership over very personal identifiers could have untold harmful consequences.

102. The Illinois legislature concluded that the increased risk of future harm is a compensable loss under the BIPA. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 35, 129 N.E.3d 1197, 1206 citing 740 ILCS § 14/5(c) (noting increased risk of identity theft should biometrics be compromised); *Dillon v. Evanston Hosp.*, 199 Ill. 2d 483, 507, 771 N.E.2d 357, 372 (2002) (Illinois Supreme Court finding risk of future injury compensable as an element of damages

in medical malpractice case). The legislature's decision is particularly reasonable given that the statute of limitations on BIPA claims presumably runs from the date of the collection of biometrics, whereas the future injury may not occur until after the statute has run.

103. Plaintiffs seek an award of liquidated damages, which is appropriate given that this harm is difficult to quantify.

104. No amount of time or money can compensate Plaintiffs if their biometric data is or has been compromised by the lax procedures through which Defendants collects, captures, obtains, stores, disseminates, and/or uses Plaintiffs' biometrics.

105. Moreover, Plaintiffs would not have provided their biometric data to Defendants if they had known that Defendants would retain such information for an indefinite period of time without their consent.

106. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). As Plaintiffs are not required to allege or prove actual damages in order to state a claim under BIPA, Plaintiffs seek statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach,* 2019 IL 123186, ¶ 40.

COUNT I

Violation of § 15(a) of BIPA
[Failure to Institute, Maintain, and Adhere to Publicly Available Retention Schedule]

107. Plaintiffs restate paragraphs 1 through 106 of the complaint as if set out here in full.

108. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention - and, importantly, deletion - policy. Specifically,

these companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 15(a).

109. Each Defendant failed to comply with these BIPA mandates.

110. Both Food 4 Less and Kroger qualify as a "private entity" under BIPA. *See* 740 § ILCS 14/10.

111. Plaintiffs are each an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendants. *See* 740 ILCS § 14/10.

112. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

113. Each Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 15(a).

114. Each Defendant failed to make any written policy establishing a retention schedule and guidelines for permanent deletion of biometric data publicly available.

115. Each Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' biometric data when the purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

116. Plaintiffs have never seen, been able to access, or been informed of any publicly available biometric data retention policy or guidelines developed by Defendants, nor have they ever seen, been able to access, or been informed of whether Defendants would ever permanently delete their biometric data.

117. Each Defendant knew, or was reckless in not knowing, that the biometric-enabled time clock system it used would be subject to the provisions of BIPA, a law in effect since 2008, yet has completely failed to comply with Section 15(a) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15(a) of BIPA.

118. Alternatively, each Defendant negligently failed to comply with Section 15(a) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(a) of BIPA.

WHEREFORE, Plaintiffs respectfully request that this Honorable Court provide each Plaintiff with the following relief:

a. Declaring that Defendants violated Section 15(a) of BIPA;

b. Requiring Defendants to comply with BIPA's requirements for the collection, otherwise obtainment, storage, use, and dissemination of biometric identifiers and biometric information as described herein;

c. Requiring Defendants to destroy biometric identifiers or biometric information pursuant to and in compliance with Section 15(a) of BIPA;

d. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(a) of BIPA pursuant to 740 ILCS § 14/20(1);

e. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(a) of BIPA pursuant to 740 ILCS § 14/20(2);

f. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

g. Enjoining Defendants from further violations of Section 15(a) of BIPA.

COUNT II

Violation of § 15(b) of BIPA
[Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information]

119. Plaintiffs restate paragraphs 1 through 106 of the complaint as if set out here in full.

120. BIPA requires companies to obtain informed written consent from its workers before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS § 14/15(b) (emphasis added).

121. "A party violates Section 15(b) when it collects, captures, or otherwise obtains a person's biometric information without prior informed consent. This is true the first time an entity scans a fingerprint or otherwise collects biometric information, but it is no less true with each subsequent scan or collection." *Cothron v. White Castle System, Inc*., 2023 IL 128004 ¶ 24 (internal citation omitted).

122. Informed consent is the "heart of BIPA." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020).

123. Each Defendant failed to comply with these BIPA mandates.

124. Both Food 4 Less and Kroger qualify as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

125. Plaintiffs are each an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant. *See* 740 ILCS § 14/10.

126. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

127. Defendants collected, captured or otherwise obtained Plaintiffs' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS § 14/15(b)(3).

128. Neither Defendant informed Plaintiffs in writing that their biometric identifier or biometric information was being collected or stored, or of the specific length of term for which their biometric identifiers and/or biometric information were being collected, stored or used before collecting, storing or using them as required by 740 ILCS § 14/15(b)(1)-(2).

129. Prior to collecting Plaintiffs' biometric identifiers and information, neither Defendant obtained a written release authorizing such collection. 740 ILCS § 14/15(b)(3).

130. By collecting, capturing, and otherwise obtaining Plaintiffs' biometric identifiers or information as described herein, each Defendant violated Plaintiffs' privacy in their biometric identifiers and information as set forth in BIPA *each time* the Defendants collected, captured, obtained, stored or used Plaintiffs' biometric identifiers or information. *See* 740 ILCS § 14/1, *et seq.*; *Cothron v. White Castle System, Inc*., 2023 IL 128004 ¶ 24. "[T]he plain language of section 15(b) and 15(d) demonstrates that such violations occur with every scan or transmission." *Id.* At ¶ 30.

131. Each Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with Section 15(b) of BIPA, or otherwise intentionally or recklessly failed to comply with Section 15(b) of BIPA.

132. Alternatively, each Defendant negligently failed to comply with Section 15(b) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(b) of BIPA.

WHEREFORE, Plaintiffs respectfully request that this Honorable Court provide each Plaintiff with the following relief:

a. Declaring that each Defendant violated Section 15(b) of BIPA;

b. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(b) of BIPA pursuant to 740 ILCS § 14/20(1);

c. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(b) of BIPA pursuant to 740 ILCS § 14/20(2);

d. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

e. Enjoining Defendants from further violations of Section 15(b) of BIPA.

COUNT III

Violation of § 15(d) of BIPA
[Disclosure of Biometric Identifiers or Information Without Obtaining Consent]

133. Plaintiffs restate paragraphs 1 through 106 of the complaint as if set out here in full.

134. BIPA prohibits private entities from disclosing, redisclosing or otherwise disseminating a person's or customer's biometric identifier or biometric information without obtaining consent for that disclosure, redisclosure or dissemination, with limited exceptions, none of which are appliable here. 740 ILCS § 14/15(d).

135. Each Defendant failed to comply with this BIPA mandate.

136. Both Food 4 Less and Kroger qualify as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

137. Plaintiffs are each an individual who had "biometric identifiers" (in the form of fingerprints) collected by Defendant, as explained in detail above. *See* 740 ILCS § 14/10.

138. Plaintiffs' biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

139. Each Defendant systematically and automatically collected, captured, or otherwise disseminated each Plaintiff's biometric identifiers and/or biometric information without obtaining the consent required by 740 ILCS § 14/15(d)(1).

140. By utilizing a biometric timekeeping system (time clock and timekeeping databases), each Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated biometric identifiers or biometric information of Plaintiffs to at least one third-party payroll company utilized by the Defendants without first obtaining the Plaintiffs' consent required by 740 ILCS § 14/15(d)(1).

141. By disclosing, redisclosing, or otherwise disseminating Plaintiffs' biometric identifiers and biometric information without his consent as described herein, each Defendant violated BIPA *each time* there was a disclosure, redisclosure or dissemination of the Plaintiffs' biometric identifiers in violation of Plaintiffs' rights to privacy in their biometric identifiers or biometric information as set forth in BIPA. *See* 740 ILCS § 14/1, *et seq*.

142. Each Defendant knew, or was reckless in not knowing, that the biometric timekeeping systems used would be subject to the provisions of BIPA, a law in effect since 2008, yet completely failed to comply with the statute, or otherwise intentionally or recklessly failed to comply with Section 15(b) of BIPA.

143. Alternatively, each Defendant negligently failed to comply with Section 15(d) of BIPA by failing to adhere to the reasonable standard of care in its industry with respect to biometric information and the mandates of Section 15(d) of BIPA.

144. "[T]he plain language of section 15(d) supports the conclusion that a claim accrues upon each transmission of a person's biometric identifier or information without prior informed consent." *White Castle System, Inc*., 2023 IL 128004 at ¶ 29.

WHEREFORE, Plaintiffs respectfully request that this Honorable Court provide each Plaintiff with the following relief:

a. Declaring that each Defendant violated Section 15(d) of BIPA;

b. Awarding liquidated damages of $1,000 for *each* negligent violation of Section 15(d) of BIPA pursuant to 740 ILCS § 14/20(1);

c. Awarding liquidated damages of $5,000 for *each* intentional and/or reckless violation of Section 15(d) of BIPA pursuant to 740 ILCS § 14/20(2);

d. Awarding reasonable attorneys' fees, costs and other litigation expenses pursuant to 740 ILCS § 14/20(3); and

e. Enjoining Defendants from further violations of Section 15(d) of BIPA.

JURY DEMAND

Plaintiffs hereby respectfully demand a trial by jury.

Respectfully submitted,

DESMOND GARMON, ZELL HATHORNE, LEWIS HOBBY, JR., BENNIE REED, RHANAE GREER, SUNSHINE SMITH, ANTWON CHERRY, CHARISSE LANGSTON, And LATONIA ADAMS

/s/ Samuel L. Eirinberg

Majdi Hijazin # 6284879
Adam J. Feuer # 6307792
Samuel L. Eirinberg # 6328842
DJC LAW, PLLC
140 S. Dearborn Street, Ste. 1610
Chicago, Illinois 60603
(872) 804-3400
sam@teamjustice.com
adam@teamjustice.com
majdi@teamjustice.com

Nick Wooten
DJC LAW, PLLC
1012 West Anderson Lane
Austin, Texas 78757
(512) 220-1800
nick@teamjustice.com

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I certify that on June 3, 2024, a copy of the foregoing First Amended Complaint was served via electronic means on:

Diane Webster (#6284225)
Richard E. Daniels (#6335759)
GORDON REES SCULLY MANSUKHANI, LLP
One North Franklin Street, Suite 800
Chicago, Illinois 60606
Tel: (312) 565-1400
dwebster@grsm.com
rdaniels@grsm.com

Counsel for Defendant

/s/ Samuel L. Eirinberg
One of the Attorneys for Plaintiffs